

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-093557

(43)Date of publication of application : 10.04.1998

(51)Int.Cl.

H04L 12/24

H04L 12/26

H04B 17/00

H04L 12/56

H04L 29/14

(21)Application number : 08-243285

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 13.09.1996

(72)Inventor : KATO TAKEHISA  
SHIMIZU HIDEO  
KITAORI MASASHI  
KAWAMURA SHINICHI  
ENDO NAOKI

(54) COMMUNICATION MONITOR DEVICE AND COMMUNICATION MONITOR METHOD

(57) [Abstract]

[PROBLEM TO BE SOLVED] To provide an encryption

5 communication system enabling efficiently and effectively monitoring a content of encrypted information transmitted from an internal network to an external network.

[SOLUTION] A communicator monitor that monitors encrypted information transmitted from a terminal belonging

10 to an internal network to be a managing target to a terminal connected via an external network, concerning information transmitted from the terminal belonging to the internal network to the terminal connected via the external network, is characterized in having a means for collecting  
15 a transmission history with a pair of a transmission source and a transmission destination as a key and a means for not transferring the information to the transmission destination and transferring to a predefined specific address when transmitting the information possessed by the  
20 pair of the transmission source and the transmission destination for which a prescribed statistic amount obtained by the collected transmission history has satisfied a prescribed condition.



## 【特許請求の範囲】

【請求項1】管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査装置において、

前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向け送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集する手段と、

収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送する手段とを備えたことを特徴とする通信監査装置。

【請求項2】前記外部ネットワークを介して接続された端末を送信先とする情報を復元して内容を監査する場合がある旨の警告文を、所定のタイミングで前記内部ネットワークに属する端末に表示させる手段を備えたことを特徴とする請求項1に記載の通信監査装置。

【請求項3】前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復元して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信する手段を備えたことを特徴とする請求項1に記載の通信監査装置。

【請求項4】管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査方法において、

前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向け送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集し、

収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送することを特徴とする通信監査方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ネットワークに接続された端末間で情報を暗号化して送受信する暗号通信システムに関する。

## 【0002】

【従来の技術】近年では、ネットワークに接続されたワークステーションやパーソナルコンピュータなどの端末間で文書・画像・音声などの情報を電子化して送受信する通信システムが広く普及している。

【0003】このような通信システムにおいて、情報の受け渡しにあたっては（特に外部のネットワークを介し

た情報の受け渡しにあたっては）、情報の秘匿性を確保するために、送信側で情報を暗号化し、受信側で暗号化された情報を復号する暗号通信を用いることが多い。すなわち、情報を暗号化してネットワークへ送信することで、送信者が宛先として指定した相手以外のネットワーク利用者にはその情報を閲覧等することができなくなり、情報の秘匿性を保つことができる。

【0004】しかしながら、ある一機りのネットワーク（例えば社内ネット）からその外部へ送り出される情報について、その情報が例えば企業秘密に関わる情報であるか否かなどについて監視しようとしても、その送り出されようとする情報を逐一復号する必要がある、監視が困難であった。

## 【0005】

【発明が解決しようとする課題】以上のように従来は、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、ある一機りのネットワークからその外部へ送り出される情報の内容を監視することが困難であった。

【0006】本発明は、上記事情を考慮してなされたもので、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、ある一機りのネットワークからその外部へ送り出される情報の内容の監視を効率的かつ効果的に行うことのできる暗号通信システムを提供することを目的とする。

## 【0007】

【課題を解決するための手段】本発明（請求項1）は、管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報（例えば、文書、画像、音声など）を監視する通信監査装置において、前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向け送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集する手段と、収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった（例えば、総転送回数がしきい値を越えるものとなった）送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送する手段とを備えたことを特徴とする。

【0008】これによって、前記情報の転送を受けた前記特定の宛先の端末を操作可能な監査人は、送信元ユーザ（または送信元ユーザと送信先ユーザの組）により特定される復号鍵を用いて該情報を復号して内容を監査することができる。

【0009】また、監査後、その内容に問題がないと判断された場合には、該特定の端末から情報をあらためて送信先に向けて送り出すようにしてもよい。あるいは、通信監査装置内に該パケットを識別子を付して保持しておき、該特定の端末から通信監査装置にパケットの識別

子を指定して該パケットをその本来の送信先に向けて送り出すよう指示を出すようにしても良い。あるいは、該情報の送信元に該情報を再度その本来の送信先に向けて送り出すよう指示を出すようにしても良い。

【0010】ここで、前記所定の条件を適宜設定することにより、監査対象を絞った効率的かつ効果的な監査を行うことができる。例えば、所定の条件を総転送回数のしきい値とすることにより、転送回数が際だって多い特定の送信元と送信先の組を持つ情報についてのみ監査対象とすることができる。

【0011】好ましくは、前記外部ネットワークを介して接続された端末を送信先とする情報を復号して内容を監査する場合がある旨の警告文を、所定のタイミングで（例えば該端末を立ち上げる際に）前記内部ネットワークに属する端末に表示させる手段を備えても良い。

【0012】これによって、該端末のユーザに警告を与え、例えば外部に企業秘密に關わる情報を漏洩するような不正を未然に防止する効果を得ることができる。好ましくは、前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復号して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信する手段を備えても良い。

【0013】これによって、該端末のユーザは、情報が送信先に転送されなかった理由が、ネットワーク上の通信エラーなどによるものではなく、監査によるものであることを知ることができる。

【0014】本発明（請求項4）は、管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査方法において、前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集し、収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報を該送信先として送り出され、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送することと特徴とする。

【0015】好ましくは、前記外部ネットワークを介して接続された端末を送信先とする情報を復号して内容を監査する場合がある旨の警告文を、所定のタイミングで前記内部ネットワークに属する端末に表示させるようにしても良い。

【0016】好ましくは、前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復号して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信するようにしても良い。なお、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

#### 【0017】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図1は、本発明の一実施形態に係る暗号通信システムを示す概念図である。図1において、内部ネットワーク11は、社内ネットワーク（企業内ネットワーク）などのローカルエリアネットワークであり、例えば会社の各部署や工場、営業所などに設置された各端末を結んでいる。なお、内部ネットワーク11は、社内ネットワークに限らず、所定の組織単位あるいは管理単位のネットワークであれば良い。

【0018】外部ネットワーク12は、内部ネットワーク11からみた外部のネットワークである。内部ネットワークを社内ネットワークとすると、外部ネットワークは社外ネットワークに相当する。外部ネットワーク12の一例としては、世界中に張り巡らされているインターネットが代表的である。

【0019】情報監査装置13は、内部ネットワーク11に属する端末を管理対象とし、内部ネットワーク11に属する端末から社外ネットワーク12に送り出される情報を監視する。本実施形態では、情報をパケット単位で監視するものとする。すなわち、情報監査装置13は、パケット内に書き込まれた送信元と送信先の情報をもとに、該パケットが内部のどのユーザを送信元として外部のどのユーザを送信先として送り出されたかを監視し、その統計情報を収集する。そして、この統計情報をもとにパケットの監査を行う。

【0020】図2に、本実施形態で転送対象となるパケットの一例としてTCP/IPパケットの構造を示す。図2に示すように、パケットには、少なくとも、送信元アドレス21、送信先アドレス22、プロトコルの種類（ポート番号）23、データの内容24が含まれるものとする。

【0021】なお、本実施形態では、パケット内に送信元となるユーザ（内部のユーザ）を特定可能なデータが含まれているものとする。例えば、送信元アドレス21で内部のユーザを特定可能とする。

【0022】本実施形態では、内部のユーザは秘密鍵暗号を用いて情報（図2ではデータの内容24）を暗号化し通信を行うものとする。内部のユーザの使用する秘密鍵は、ユーザをキーとしてあるユーザとその通信相手の組をキーとして、内部ネットワーク11内で管理されているものとする。秘密鍵暗号については、池野、小山共著「現代暗号理論」電子情報通信学会編や、岡本著「暗号理論入門」共立出版株式会社等に詳しいので、ここでの説明は省略する。

【0023】次に、通信監査装置20の機能について説明する。通信監査装置20は、内部のユーザから外部への送信の状況を、パケットの送信元アドレス21と送信先アドレス22を参照して統計処理により把握する。そして、所定の統計量が予め定められた所定の条件を満

たものになると（例えば転送パケットの累計数がしきい値以上になると）、パケットをその本来の送信先へは転送せずに、パケット内の暗号化された情報を復号しその内容の監査を行うために該パケットを監査人（すなわち、内部の特定のユーザ）宛てに転送する。

【0024】以下、具体例として発信された電子メールを監査する場合について説明する。図3に、通信監査装置20による監査の概要を示す。図3において、ユーザAを監査人、ユーザBを内部のユーザ（例えば社員）とし、ユーザCとユーザDが外部のユーザ（例えば社外のユーザ）であるとする。

【0025】通信監査装置20は、内部のユーザBから外部のユーザC宛てあるいはユーザD宛てのパケットを受け取ると、パケット内に記述されている送信元アドレスと送信先アドレスを調べ、送信元と送信先の組ごとにパケット量を累計して行く。

【0026】図3では、ユーザBの通信記録として、C宛てにx回、D宛てにy回、パケット転送が行われた状態が示されている。ここで、例えば、上記所定の条件を「今受け取ったパケットをその宛先に転送すると通信回数がx（ここで $x > y$ とする）回を越える」条件であるとする。この場合、図3の状態でユーザBからD宛てにパケットが送信されると、該パケットはこの条件を満たさないで、通信監査装置20はD宛てにパケットを送り出す（D宛ての通信回数は $y+1$ となる）。一方、図3の状態でユーザBからC宛てに送信されたパケットが通信監査装置20に入力されると、C宛ての通信回数は $x+1$ にカウントアップされ、この結果、該パケットは上記条件を満たすことになるので、通信監査装置20は、該パケットをC宛てには転送せずに、監査人Aの端

末宛てに転送する。

【0027】このようにして上記パケットを転送された監査人Aは、送信元アドレス（または送信元アドレスと送信先アドレスの組）により特定される秘密鍵を用いて該パケット内の暗号化データを復号して内容を監査することができる。なお、該秘密鍵は、監査人Aの端末あるいはこれに直接接続されたサーバあるいは内部ネットワーク11内の他のサーバ装置で管理し、監査人Aの端末にて入手可能であるものとする。

【0028】また、監査後、その内容に問題がないと判断された場合には、該監査人Aの端末からパケットをあらためて本来の送信先に向けて送り出すようにしても良い。あるいは、通信監査装置20内に該パケットを識別子を付して保持しておき、該監査人Aの端末から通信監査装置20にパケットの識別子を指定して該パケットをその本来の送信先に向けて送り出すよう指示を出すようにしても良い。あるいは、該パケットの送信元と該パケットを再度その本来の送信先に向けて送り出すよう指示を出すようにしても良い。

【0029】ここで、前記所定の条件を適宜設定するこ

とにより、監査対象を絞った効率的かつ効果的な監査を行うことができる。例えば、所定の条件を総転送回数のしきい値とすることにより、転送回数が際だって多い特定の送信元と送信先の組を持つ情報についての監査対象とすることができる。

【0030】次に、図4に、通信監査装置20の内部構成の一例を示す。また、図5に、通信監査装置20の処理の流れの一例を示す。通信監査装置20は、パケット解析部43、送信ログ取得部45、送信パケット統計処理部46、監査条件判定部47、メール発信部48を備えている。

【0031】図4において、41はユーザBからの暗号メールを示し、42は送信されるパケットに含まれる情報の概略を示している。まず、暗号メールを受信すると、パケット解析部43でパケット内に記述された該パケットの送信元と送信先を検出する（ステップS11）。また、必要に応じて、プロトコルの種類、データ量など、他の情報も検出する。

【0032】次に、送信ログ取得部45は、パケットの送信元と送信先の組ごとにログを取る。ログの内容は、例えば、日時、送信元、送信先、プロトコルの種類などからなる。あるいは、データ量などを付加しても良い。

【0033】次に、送信パケット統計処理部46は、送信ログ取得部45からの情報をもとに、パケット毎に統計処理を行う（ステップS12）。ここでは、送信元と送信先の組ごとにパケット数を計数するものとする。なお、送信元と送信先とプロトコルの種類の組ごとに統計処理を行っても良いし、特定の種類のプロトコルについてのみ、送信元と送信先の組ごとにパケット数の計数するようにしても良いし、その他、種々の統計処理の方法が考えられる。

【0034】なお、送信ログ取得部45を設けない構成も考えられる。この場合、パケット解析部43から直接、送信パケット統計処理部46に、必要なデータを与える。次に、監査条件判定部47は、パケット毎に行った統計処理により得られる所定の統計量が、予め定めた条件を満たすか否かを判定する（ステップS13）。

【0035】ここでは、一例として、所定の統計量を送信回数 $n$ とし、予め定めた条件を「送信回数 $n$ がしきい値 $N$ 以上であること」とする。この場合、監査条件判定部47は、暗号メールを監査するか否かを決定するためのしきい値 $N$ と送信回数 $n$ を比較する。

【0036】上記条件が満たされない場合（本具体例では $N > n$ である場合）には（ステップS14）、監査すべき条件が満たされないで、該電子メールを本来の送信先に向けて外部ネットワーク12に送り出す（ステップS15）。

【0037】一方、上記条件が満たされる場合（本具体例では $N \leq n$ である場合）には（ステップS14）、監査すべき条件が満たされるので、メール発信部48は、

このメールを監査人Aに発信する(ステップS16)。

【0038】なお、通信監査装置20内では、パケットを送信するまでバッファに蓄積しておいても良いし、パケット解析部43、送信ログ取得部45、送信パケット統計処理部46、監査条件判定部47、メール発信部48の各部分でリレーして言うても良い。

【0039】以下、具体例を用いて通信監査装置20の動作例を説明する。今、図3のユーザBが暗号メールをユーザC宛てに送信したとする。ユーザBが発信した暗号メールは、パケットとして図4中の42に示すように発信元および発信先がヘッダとして付加される。

【0040】このパケットを受け取った通信監査装置20では、パケット解析部43により該パケットがユーザBからのパケットであること、該パケットがユーザCへ発信されていることなどを検出し、その結果を送信ログ取得部45へ送る。

【0041】送信ログ取得部45は、送信元と送信先とを組にして、パケット送信のログを記録しておく。本具体例では、ユーザBがパケットをユーザCに送信したログを記録しておく。

【0042】この結果を、送信パケット統計処理部46へ送り、ある特定のパケット、例えば現在送信されているパケットのこのまでの個数をカウントする。この結果を、nとする。

【0043】このnを監査条件判定部47へ送り、あるしきい値Nと比較する。このしきい値は、監査人Aが予め設定した値である。このとき、nがしきい値N未満である場合は、該パケットをユーザCに向けて外部ネットワーク12に送り出す。

【0044】一方、nがしきい値N以上となった場合は、メール発信部48にて、ユーザBが送信した暗号メールを監査人Aへ送信する。なお、同時に、ユーザBからユーザCへのパケットの量がしきい値N以上となったことをメールにて知らせるようにしても良い。

【0045】この結果、監査人Aは、ユーザBから出されたユーザC宛ての暗号メールを、所定の鍵で復号し内容を監査することができる。また、メール発信部48は、ある特定の内容を持つパケット、例えば使用されていないポート番号を付加したパケットをユーザBのホストマシンへ送信する。ユーザBのホストマシンは、警告メッセージ発信部49でこの特定のパケットを受け取り、警告メッセージをユーザBが使用しているマシンのディスプレイ上に、例えば、「これより暗号化されたメールの監査を行います」というメッセージとして表示するようにしても良い。この警告メッセージは、現在使われているファイアウォールの警告システムと同様に、各ホストマシンにソフトウェアで実現可能である。

【0046】なお、以上では、所定の統計量としてパケット数、所定の条件として「パケット数がしきい値以上になること」を一例として示したが、これに限定される

ものではない。

【0047】例えば、監査対象とする送信元の範囲、あるいは送信先の範囲、あるいは送信元と送信先の組の範囲を限定しても良い。また、上記所定の条件あるいは所定の統計量および所定の条件を、送信元、あるいは送信先、あるいは送信元と送信先の組ごとに設定しても良い。

【0048】また、上記所定の統計量を一定期間毎に求めても良い。例えば、転送パケット数を月初めにクリアし、当該月における転送パケット数としきい値を比較するようにしても良いし、その日から過去一定期間の間の転送パケット数で比較するようにしても良い。

【0049】その他、種々変形して実施可能である。なお、以上では、監査するパケットを監査人に転送していたが、その代わり、パケットは監査人に転送せずに、監査人にメッセージのみ転送するようにしても良い。この場合にも、監査人は、通信監査装置内に保持されているパケットを監査することができる。

【0050】ところで、内部のユーザが、自分のホストマシンを立ち上げ、マシンにログインをすると、画面上に、例えば「本システムを使用して外部へ情報を暗号化して送信する場合、復号して情報の内容を監査することがあります。」というメッセージを表示させるようにしても良い。

【0051】これによって、該端末のユーザに警告を与え、例えば外部に企業秘密に関わる情報を漏洩するような不正を心理的に抑え未然に防止する効果を得ることができる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0052】

【発明の効果】本発明によれば、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、送信履歴をもとにして一定の条件を成立させる情報を監査対象として選択することで、内部ネットワークからその外部へ送り出される情報の内容の監視を効率的かつ効果的に行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る暗号通信システムの概念を示す図

【図2】同実施形態におけるパケットの構造の一例を示す図

【図3】同実施形態の通信監査装置の動作を説明するための図

【図4】同実施形態の通信監査装置の内部構成の一例を示す図

【図5】同実施形態の通信監査装置の処理の流れの一例を示すフローチャート

【符号の説明】

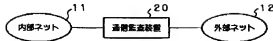
11…社外ネットワーク

- 12…社内ネットワーク  
13…通信監査装置  
35…通信監査装置  
43…パケット解析部  
45…送信ログ取得部

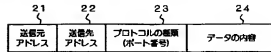
\*

- \* 46…送信パケット統計処理部  
47…監査条件判定部  
48…メール発信部  
49…警告メッセージ表示部

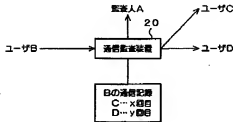
【図1】



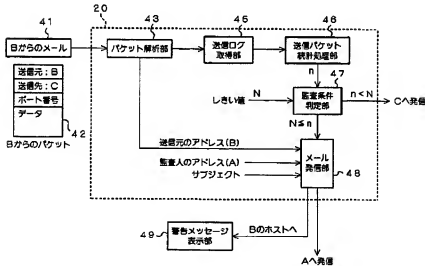
【図2】



【図3】

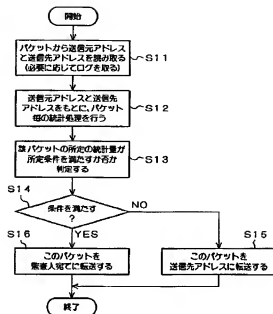


【図4】





【図5】




---

フロントページの続き

(72)発明者 川村 信一  
神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 遠藤 直樹  
神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内